What is claimed is:

1. A system for downloading encrypted electronic information from a host device to a gaming terminal through a communications link between said host device and said terminal, wherein said terminal comprises a decryption component configured for decrypting said encrypted electronic information using at least two security keys, at least one said key being resident in said terminal and at least another said key being delivered to said terminal at the time of said downloading, and wherein said downloading facilitates a replacement of electronic information stored in said terminal with corresponding decrypted information obtained from decrypting said encrypted information, said downloading system comprising:

(a) a host component configured for transmitting said encrypted electronic information from said host device to said terminal, wherein said encrypted information comprises at least one next version key for later use by said decryption component in decrypting a next version of encrypted electronic information;

(b) a receiving component configured for receiving said encrypted information by said terminal; and,

(c) delivery means configured for delivering said other key to said terminal at the time of said downloading.

2. A system according to claim 1 wherein said encrypted electronic information is in the form of packs, said packs comprising a full set of files for updating said terminal's software.

3. A system according to claim 2 wherein said communications link comprises a cable coupled to parallel ports of said host and terminal and said delivery means comprises an electronic security key.

4. A system according to claim 3 wherein said encrypted information

comprises assigned bit information associated with a next version electronic key, said bit information being for later use with said delivery means to deliver said other security key for use by said decryption component in decrypting a next version of encrypted electronic information.

5. A system according to claim 4 wherein said cable is wired to provide crossed control lines and bidirectional communications for data transfer.

6. A system according to claim 5 wherein said electronic security key is configured for providing means for decrypting an encrypted master reset component in said terminal.

7. A system according to claim 6 wherein said electronic security key comprises information usable by said terminal to distinguish the electronic information version that different electronic keys are configured for.

8. A system according to claim 6 wherein said delivery means comprises a secure network.

9. A system according to claim 8 wherein said network is a wide area ethernet network.

10. A system according to claim 4 wherein said files are stored in said terminal in nonvolatile memory following decryption of said packs.

11. A system according to claim 9 wherein said files are stored in said terminal in nonvolatile memory following decryption of said packs.

12. A method for downloading encrypted electronic information from a host

device to a gaming terminal through a communications link between said host device and said terminal, whereby said terminal comprises a decryption component configured for decrypting said encrypted electronic information using at least two security keys, at least one said key being resident in said terminal and at least another said key being delivered to said terminal at the time of said downloading, and whereby said downloading facilitates a replacement of electronic information stored in said terminal with corresponding decrypted information obtained from decrypting said encrypted information, said downloading method comprising:

(a) transmitting said encrypted electronic information from said host device to said terminal, whereby said encrypted information comprises at least one next version key for later use by said decryption component in decrypting a next version of encrypted electronic information;

(b) receiving said encrypted information at said terminal; and,

(c) delivering said other key to said terminal at the time of said downloading.

13. A method according to claim 12 whereby said encrypted electronic information is in the form of packs, said packs comprising a full set of files for updating said terminal's software.

14. A method according to claim 13 whereby said communications link comprises a cable coupled to parallel ports of said host and terminal and said delivering comprises providing an electronic security key to said terminal.

15. A method according to claim 14 whereby said encrypted information comprises assigned bit information associated with a next version electronic key, said bit information being for later use for delivering said other security key for use by said decryption component in decrypting a next version of encrypted electronic information.

16. A method according to claim 15 whereby communications through said

communications link are bidirectional.

17. A method according to claim 16 and further comprising providing in said electronic security key means for decrypting an encrypted master reset component in said terminal.

18. A method according to claim 16 and further comprising providing in said electronic security key information usable by said terminal to distinguish the electronic information version that different electronic keys are configured for.

19. A method according to claim 13 whereby said communications link is a secure network and said delivering is performing by means of said network.

20. A method according to claim 19 whereby said network is a wide area ethernet network.